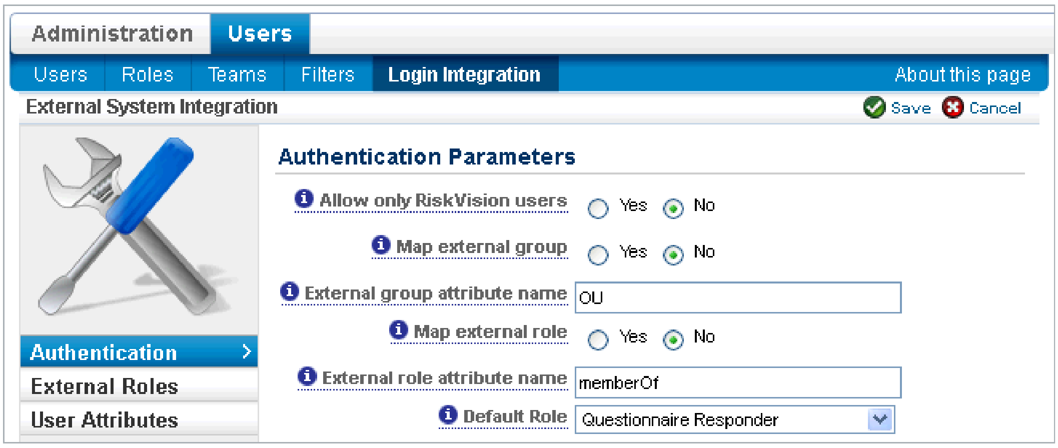
Establishing and Managing Roles

In RiskVision, new users can be created manually or by importing them. When SAML has been configured properly, a user will be automatically created in RiskVision when logging in through an identity provider for the first time. Newly created users will be assigned the default role that has been set in the **Login Integration** tab of the **Users** menu.



External System Integration

Authentication Parameters

Allow only RiskVision users ○ Yes ● No

Map external group ○ Yes ● No

External group attribute name: OU

Map external role ○ Yes ● No

External role attribute name: memberOf

Default Role: Questionnaire Responder

The Login Integration tab of the Useers Menu in RiskVision.

A SAML user that has been assigned to the **administrator** role can perform user management tasks such as importing users, changing the default tole in the **Login Integration** tab, and changing the roles and permissions for users in general.

If at least one SAML user has not been granted an **administrator** role, a system administrator must bypass the normal SAML SSO login in order to grant access.

To bypass the SAML SSO login:

1. Disable SAML by reverting the **applicationContext-security.xml** file to its original settings before you configured it.

2. Restart Tomcat to put the above changes into effect.

3. Log in to RiskVision.

4. Access the **Administration** application to assign roles and permissions to the SAML users. Ensure that one or more SAML users has been assigned to the **administrator** role.

5. Reconfigure the **applicationContext-security.xml** file to enable users to login using SAML SSO.